Mobile Device Policy

Version 3.0

12th February 2020

Rue des Oursins, 21731, Baie du Tombeau I T : +(230) 206 8200 I F : +(230) 247 1010 I E : corporate@lasentinelle.mu

Document History

Created by:	Eddy Lareine
Approved by:	Areff Salauroo

Release date	Version	Change Details	Reviewed by
22.10.19	1.0	Submitted for review	Legal Advisor
12.11.19	2.0	Apply changes submitted by legal advisor	Eddy Lareine
12.02.20	3.0	Submitted for review	Areff Salauroo

Table of Contents

MOBILE DEVICE POLICY

1.0 Objective

The purpose of this policy is to: -

- Define and set out the appropriate use of mobile devices;
- Ensure the protection of information held on or accessible from mobile devices;
- Ensure that risks introduced by using mobile devices are properly managed and mitigated;
- Minimise the threat of accidental, unauthorised or inappropriate access to electronic information through the use of mobile devices;
- Provide guidelines for acceptable use of mobile devices.

2.0 Scope

This policy applies to all La Sentinelle Ltd employees using company owned or authorized personal mobile devices which are capable of storing and transmitting information owned by the Company.

3.0 References to IS0 27001:2013

- **Mobile Device Policy - A.6.2.1**

  A policy and supporting security measures shall be adopted to manage risks introduced by using mobile devices.

4.0 Definitions

i. LSL network – La Sentinelle Ltd LAN (Local Area Network) and WAN (Wide Area Network) infrastructure that provide connectivity to La Sentinelle Ltd Corporate Services.
ii. Corporate connectivity – A connection that provides access to La Sentinelle Ltd network.
iii. MAC address – The MAC address is a hardware number that uniquely identifies each node on a network and is required for every port or device that connects to the network.
iv. Mobile devices - Mobile computing and/or Communications Devices, for example, laptops/notebooks, handheld wireless devices, smart phones, tablets, etc.
v. Clear-text – Unencrypted data.
vi. Full disk encryption – Technique that encrypts an entire hard drive, including operating system and data
vii. Key – Phrase used to encrypt or decrypt data.
viii. Remote wipe – Software that remotely deletes data stored on a mobile device.

5.0 Policy Description

Mobile devices will be issued only to La Sentinelle Ltd personnel with duties that require them to be in immediate and frequent contact with company resources and information, when they are away from their normal work locations.

5.1 Protection of La Sentinelle Ltd Data

The following measures are taken to protect La Sentinelle Ltd data:

a) Prior to initial use on the company's network or related infrastructure, all mobile devices must be registered with and authorised by La Sentinelle Ltd IT Department. The IT Department will maintain a list of approved mobile devices and related software applications and utilities as needed. Devices that are not on this list may not be connected to La Sentinelle Ltd infrastructure. Although IT currently allows only listed devices to be connected to the company's infrastructure, it reserves the right to update this list in the future.

b) On termination of an employee, all mobile devices will be de-registered and access to corporate network and resources will be revoked by La Sentinelle Ltd IT Department.

c) Laptop computers or personal PCs may only access the company's network using a Virtual Private Network (VPN) connection.

d) Mobile Devices must be configured with a secure password that complies with La Sentinelle Ltd Password Policy.

e) Information security training and awareness sessions on the additional risks associated with Mobile Devices are arranged for applicable employees.

f) La Sentinelle Ltd confidential or secret data may not be stored on Mobile Devices unless protected by approved encryption.

g) Users are expressly forbidden from storing La Sentinelle Ltd data on devices that are not issued by La Sentinelle Ltd such as storing La Sentinelle Ltd email on a personal MCCD.

h) Backups of important information are taken regularly in line with the La Sentinelle Ltd Backup Policy.

i) Mobile devices are physically protected against theft.

j) Mobile devices carrying important, sensitive, and/or critical business information are not to be left unattended in line with the company's Asset Policy, Acceptable Use Policy and Equipment Security Policy.

k) Users must only load data essential to their role onto their Mobile Devices.

l) Users must report all lost or stolen devices to the Head of IT of La Sentinelle Ltd, immediately.

m) If a user suspects that unauthorized access to the company data has taken place via a mobile device, the user must report the incident immediately to the Head of IT of La Sentinelle Ltd.

n) Users must not load pirated software or illegal content onto their Mobile Devices.

o) Applications must only be installed from official platform-owner approved sources. Installation of code from un-trusted sources is forbidden.

p) Devices must be kept up to date with manufacturer or network provided patches. As a minimum patch should be checked for weekly and applied at least once a month.

5.2 Laptops

Laptops must employ encryption with an approved software encryption package. No La Sentinelle Ltd secret or confidential data may exist on a laptop in clear-text.

5.3 PDAs and Cell Phones

Any La Sentinelle Ltd secret or confidential data stored on Mobile Devices must be saved to an encrypted file system using La Sentinelle Ltd approved software. La Sentinelle Ltd shall also employ remote wipe technology to remotely disable and delete any data stored on La Sentinelle Ltd PDA or cell phone which is reported lost or stolen.

5.4 Keys

All keys used for encryption and decryption must meet complexity requirements described in La Sentinelle Ltd Password Policy.

5.5 Loss and Theft

Charges for repair due to misuse of equipment or misuse of services may be the responsibility of the employee, as determined on a case-to-case basis. The cost of any item beyond the standard authorized equipment is also the responsibility of the employee. Lost or stolen equipment must immediately be reported to the Head of IT of La Sentinelle Ltd.

5.6 Personal Use

Mobile Devices are issued for La Sentinelle Ltd business purpose. Personal use should be limited to minimal and incidental use only.

5.7 General Network Access Requirements

All wireless devices that reside at La Sentinelle sites and connect to the company's network, or provide access to information classified as confidential or secret must:

a) Abide by the applicable company policies.

b) Be installed, supported, and maintained by La Sentinelle Ltd IT personnel.

c) Use La Sentinelle Ltd approved authentication and encryption protocols.

d) Maintain a MAC address that can be registered and tracked.

e) Remote Access to the corporate network through the mobile device must use standard remote access authentication.

6.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action that leads to being ineligible for continued use of Mobile Devices, up to and including termination of employment.

7.0 Employee Declaration

I have read and I understand the above Mobile Device Policy, and consent to adhere to the rules outlined therein.

Name : _____

Signature : _____

Date : _____